

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification: H02H 3/05, G06F 15/177, H04L 1/22	A1	(11) International Publication Number: WO 00/51216 (43) International Publication Date: 31 August 2000 (31.08.2000)
(21) International Application Number: PCT/US00/05086 (22) International Filing Date: 24 February 2000 (24.02.2000) (30) Priority Data: 09/258,028 25 February 1999 (25.02.1999) US (60) Parent Application or Grant LODGENET ENTERTAINMENT CORPORATION [/]; (). SLEMMER, Michael, W. [/]; (). ZINGER, David, F. ; ().		Published
(54) Title: METHOD AND APPARATUS FOR PROVIDING UNINTERRUPTED COMMUNICATION OVER A NETWORK LINK (54) Titre: PROCEDE ET APPAREIL ASSURANT UNE COMMUNICATION ININTERROMPUE SUR UNE LIAISON DE RESEAU		
(57) Abstract <p>A system for providing uninterrupted communication over a network link includes a multi-port switch that is connected to a first network portion and a second network portion (Fig. 1) that are communicating with one another. The multi-port switch is also connected to a separate server unit, such as a firewall computer. The switch is configured to direct communication signals flowing between the first network portion and the second network (Fig. 1) portion through the separate server unit for processing during normal operation. When the separate server unit fails, however, the switch is reconfigured so that communications bypass the separate server unit. In a preferred embodiment, a Ethernet switch having virtual local area network (VLAN) capability is used.</p> (57) Abrégé <p>L'invention concerne un système assurant une communication ininterrompue sur une liaison de réseau, qui comporte un commutateur multi-accès relié à une première partie du réseau et à une deuxième partie du réseau (Fig. 1) qui communiquent entre elles. Le commutateur multi-accès est également relié à un serveur distinct, tel qu'un ordinateur pare-feu. Le commutateur est configuré pour diriger des signaux de communication entre la première partie du réseau et la deuxième partie du réseau (Fig. 1) par l'intermédiaire du serveur distinct en vue d'un traitement, lors d'une exploitation normale. Cependant, en cas de défaillance du serveur, le commutateur est reconfiguré de sorte que les communications contournent ce serveur distinct. Dans un mode de réalisation préféré, on utilise un commutateur Ethernet possédant une capacité de réseau local virtuel (VLAN).</p>		

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : H02H 3/05, H04L 1/22, G06F 15/177	A1	(11) International Publication Number: WO 00/51216 (43) International Publication Date: 31 August 2000 (31.08.00)
(21) International Application Number: PCT/US00/05086 (22) International Filing Date: 24 February 2000 (24.02.00) (30) Priority Data: 09/258,028 25 February 1999 (25.02.99) US (71) Applicant: LODGENET ENTERTAINMENT CORPORATION [US/US]; 3900 West Innovation Street, Sioux Falls, SD 57107 (US). (72) Inventor: SLEMMER, Michael, W.; Apartment 310, 400 East 13th Street, Sioux Falls, SD 57104 (US). (74) Agents: ZINGER, David, F. et al.; Sheridan Ross P.C., Suite 1200, 1560 Broadway, Denver, CO 80202-5141 (US).	(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW. ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>	
(54) Title: METHOD AND APPARATUS FOR PROVIDING UNINTERRUPTED COMMUNICATION OVER A NETWORK LINK		
(57) Abstract <p>A system for providing uninterrupted communication over a network link includes a multi-port switch that is connected to a first network portion and a second network portion (Fig. 1) that are communicating with one another. The multi-port switch is also connected to a separate server unit, such as a firewall computer. The switch is configured to direct communication signals flowing between the first network portion and the second network (Fig. 1) portion through the separate server unit for processing during normal operation. When the separate server unit fails, however, the switch is reconfigured so that communications bypass the separate server unit. In a preferred embodiment, a Ethernet switch having virtual local area network (VLAN) capability is used.</p> <div data-bbox="527 1186 1282 1333"><pre>graph LR; 10[PUBLIC NETWORK] <--> 14[]; 14 <--> 12[PRIVATE NETWORK];</pre></div>		

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

Description

5

10

15

20

25

30

35

40

45

50

55

5
10
METHOD AND APPARATUS FOR PROVIDING UNINTERRUPTED
COMMUNICATION OVER A NETWORK LINK

15
20
FIELD OF THE INVENTION

The invention relates generally to communication networks and, more specifically, to devices for ensuring uninterrupted service in a communication network.

25
30
BACKGROUND OF THE INVENTION

35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995
1000
1005
1010
1015
1020
1025
1030
1035
1040
1045
1050
1055
1060
1065
1070
1075
1080
1085
1090
1095
1100
1105
1110
1115
1120
1125
1130
1135
1140
1145
1150
1155
1160
1165
1170
1175
1180
1185
1190
1195
1200
1205
1210
1215
1220
1225
1230
1235
1240
1245
1250
1255
1260
1265
1270
1275
1280
1285
1290
1295
1300
1305
1310
1315
1320
1325
1330
1335
1340
1345
1350
1355
1360
1365
1370
1375
1380
1385
1390
1395
1400
1405
1410
1415
1420
1425
1430
1435
1440
1445
1450
1455
1460
1465
1470
1475
1480
1485
1490
1495
1500
1505
1510
1515
1520
1525
1530
1535
1540
1545
1550
1555
1560
1565
1570
1575
1580
1585
1590
1595
1600
1605
1610
1615
1620
1625
1630
1635
1640
1645
1650
1655
1660
1665
1670
1675
1680
1685
1690
1695
1700
1705
1710
1715
1720
1725
1730
1735
1740
1745
1750
1755
1760
1765
1770
1775
1780
1785
1790
1795
1800
1805
1810
1815
1820
1825
1830
1835
1840
1845
1850
1855
1860
1865
1870
1875
1880
1885
1890
1895
1900
1905
1910
1915
1920
1925
1930
1935
1940
1945
1950
1955
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
2030
2035
2040
2045
2050
2055
2060
2065
2070
2075
2080
2085
2090
2095
2100
2105
2110
2115
2120
2125
2130
2135
2140
2145
2150
2155
2160
2165
2170
2175
2180
2185
2190
2195
2200
2205
2210
2215
2220
2225
2230
2235
2240
2245
2250
2255
2260
2265
2270
2275
2280
2285
2290
2295
2300
2305
2310
2315
2320
2325
2330
2335
2340
2345
2350
2355
2360
2365
2370
2375
2380
2385
2390
2395
2400
2405
2410
2415
2420
2425
2430
2435
2440
2445
2450
2455
2460
2465
2470
2475
2480
2485
2490
2495
2500
2505
2510
2515
2520
2525
2530
2535
2540
2545
2550
2555
2560
2565
2570
2575
2580
2585
2590
2595
2600
2605
2610
2615
2620
2625
2630
2635
2640
2645
2650
2655
2660
2665
2670
2675
2680
2685
2690
2695
2700
2705
2710
2715
2720
2725
2730
2735
2740
2745
2750
2755
2760
2765
2770
2775
2780
2785
2790
2795
2800
2805
2810
2815
2820
2825
2830
2835
2840
2845
2850
2855
2860
2865
2870
2875
2880
2885
2890
2895
2900
2905
2910
2915
2920
2925
2930
2935
2940
2945
2950
2955
2960
2965
2970
2975
2980
2985
2990
2995
3000
3005
3010
3015
3020
3025
3030
3035
3040
3045
3050
3055
3060
3065
3070
3075
3080
3085
3090
3095
3100
3105
3110
3115
3120
3125
3130
3135
3140
3145
3150
3155
3160
3165
3170
3175
3180
3185
3190
3195
3200
3205
3210
3215
3220
3225
3230
3235
3240
3245
3250
3255
3260
3265
3270
3275
3280
3285
3290
3295
3300
3305
3310
3315
3320
3325
3330
3335
3340
3345
3350
3355
3360
3365
3370
3375
3380
3385
3390
3395
3400
3405
3410
3415
3420
3425
3430
3435
3440
3445
3450
3455
3460
3465
3470
3475
3480
3485
3490
3495
3500
3505
3510
3515
3520
3525
3530
3535
3540
3545
3550
3555
3560
3565
3570
3575
3580
3585
3590
3595
3600
3605
3610
3615
3620
3625
3630
3635
3640
3645
3650
3655
3660
3665
3670
3675
3680
3685
3690
3695
3700
3705
3710
3715
3720
3725
3730
3735
3740
3745
3750
3755
3760
3765
3770
3775
3780
3785
3790
3795
3800
3805
3810
3815
3820
3825
3830
3835
3840
3845
3850
3855
3860
3865
3870
3875
3880
3885
3890
3895
3900
3905
3910
3915
3920
3925
3930
3935
3940
3945
3950
3955
3960
3965
3970
3975
3980
3985
3990
3995
4000
4005
4010
4015
4020
4025
4030
4035
4040
4045
4050
4055
4060
4065
4070
4075
4080
4085
4090
4095
4100
4105
4110
4115
4120
4125
4130
4135
4140
4145
4150
4155
4160
4165
4170
4175
4180
4185
4190
4195
4200
4205
4210
4215
4220
4225
4230
4235
4240
4245
4250
4255
4260
4265
4270
4275
4280
4285
4290
4295
4300
4305
4310
4315
4320
4325
4330
4335
4340
4345
4350
4355
4360
4365
4370
4375
4380
4385
4390
4395
4400
4405
4410
4415
4420
4425
4430
4435
4440
4445
4450
4455
4460
4465
4470
4475
4480
4485
4490
4495
4500
4505
4510
4515
4520
4525
4530
4535
4540
4545
4550
4555
4560
4565
4570
4575
4580
4585
4590
4595
4600
4605
4610
4615
4620
4625
4630
4635
4640
4645
4650
4655
4660
4665
4670
4675
4680
4685
4690
4695
4700
4705
4710
4715
4720
4725
4730
4735
4740
4745
4750
4755
4760
4765
4770
4775
4780
4785
4790
4795
4800
4805
4810
4815
4820
4825
4830
4835
4840
4845
4850
4855
4860
4865
4870
4875
4880
4885
4890
4895
4900
4905
4910
4915
4920
4925
4930
4935
4940
4945
4950
4955
4960
4965
4970
4975
4980
4985
4990
4995
5000
5005
5010
5015
5020
5025
5030
5035
5040
5045
5050
5055
5060
5065
5070
5075
5080
5085
5090
5095
5100
5105
5110
5115
5120
5125
5130
5135
5140
5145
5150
5155
5160
5165
5170
5175
5180
5185
5190
5195
5200
5205
5210
5215
5220
5225
5230
5235
5240
5245
5250
5255
5260
5265
5270
5275
5280
5285
5290
5295
5300
5305
5310
5315
5320
5325
5330
5335
5340
5345
5350
5355
5360
5365
5370
5375
5380
5385
5390
5395
5400
5405
5410
5415
5420
5425
5430
5435
5440
5445
5450
5455
5460
5465
5470
5475
5480
5485
5490
5495
5500
5505
5510
5515
5520
5525
5530
5535
5540
5545
5550
5555
5560
5565
5570
5575
5580
5585
5590
5595
5600
5605
5610
5615
5620
5625
5630
5635
5640
5645
5650
5655
5660
5665
5670
5675
5680
5685
5690
5695
5700
5705
5710
5715
5720
5725
5730
5735
5740
5745
5750
5755
5760
5765
5770
5775
5780
5785
5790
5795
5800
5805
5810
5815
5820
5825
5830
5835
5840
5845
5850
5855
5860
5865
5870
5875
5880
5885
5890
5895
5900
5905
5910
5915
5920
5925
5930
5935
5940
5945
5950
5955
5960
5965
5970
5975
5980
5985
5990
5995
6000
6005
6010
6015
6020
6025
6030
6035
6040
6045
6050
6055
6060
6065
6070
6075
6080
6085
6090
6095
6100
6105
6110
6115
6120
6125
6130
6135
6140
6145
6150
6155
6160
6165
6170
6175
6180
6185
6190
6195
6200
6205
6210
6215
6220
6225
6230
6235
6240
6245
6250
6255
6260
6265
6270
6275
6280
6285
6290
6295
6300
6305
6310
6315
6320
6325
6330
6335
6340
6345
6350
6355
6360
6365
6370
6375
6380
6385
6390
6395
6400
6405
6410
6415
6420
6425
6430
6435
6440
6445
6450
6455
6460
6465
6470
6475
6480
6485
6490
6495
6500
6505
6510
6515
6520
6525
6530
6535
6540
6545
6550
6555
6560
6565
6570
6575
6580
6585
6590
6595
6600
6605
6610
6615
6620
6625
6630
6635
6640
6645
6650
6655
6660
6665
6670
6675
6680
6685
6690
6695
6700
6705
6710
6715
6720
6725
6730
6735
6740
6745
6750
6755
6760
6765
6770
6775
6780
6785
6790
6795
6800
6805
6810
6815
6820
6825
6830
6835
6840
6845
6850
6855
6860
6865
6870
6875
6880
6885
6890
6895
6900
6905
6910
6915
6920
6925
6930
6935
6940
6945
6950
6955
6960
6965
6970
6975
6980
6985
6990
6995
7000
7005
7010
7015
7020
7025
7030
7035
7040
7045
7050
7055
7060
7065
7070
7075
7080
7085
7090
7095
7100
7105
7110
7115
7120
7125
7130
7135
7140
7145
7150
7155
7160
7165
7170
7175
7180
7185
7190
7195
7200
7205
7210
7215
7220
7225
7230
7235
7240
7245
7250
7255
7260
7265
7270
7275
7280
7285
7290
7295
7300
7305
7310
7315
7320
7325
7330
7335
7340
7345
7350
7355
7360
7365
7370
7375
7380
7385
7390
7395
7400
7405
7410
7415
7420
7425
7430
7435
7440
7445
7450
7455
7460
7465
7470
7475
7480
7485
7490
7495
7500
7505
7510
7515
7520
7525
7530
7535
7540
7545
7550
7555
7560
7565
7570
7575
7580
7585
7590
7595
7600
7605
7610
7615
7620
7625
7630
7635
7640
7645
7650
7655
7660
7665
7670
7675
7680
7685
7690
7695
7700
7705
7710
7715
7720
7725
7730
7735
7740
7745
7750
7755
7760
7765
7770
7775
7780
7785
7790
7795
7800
7805
7810
7815
7820
7825
7830
7835
7840
7845
7850
7855
7860
7865
7870
7875
7880
7885
7890
7895
7900
7905
7910
7915
7920
7925
7930
7935
7940
7945
7950
7955
7960
7965
7970
7975
7980
7985
7990
7995
8000
8005
8010
8015
8020
8025
8030
8035
8040
8045
8050
8055
8060
8065
8070
8075
8080
8085
8090
8095
8100
8105
8110
8115
8120
8125
8130
8135
8140
8145
8150
8155
8160
8165
8170
8175
8180
8185
8190
8195
8200
8205
8210
8215
8220
8225
8230
8235
8240
8245
8250
8255
8260
8265
8270
8275
8280
8285
8290
8295
8300
8305
8310
8315
8320
8325
8330
8335
8340
8345
8350
8355
8360
8365
8370
8375
8380
8385
8390
8395
8400
8405
8410
8415
8420
8425
8430
8435
8440
8445
8450
8455
8460
8465
8470
8475
8480
8485
8490
8495
8500
8505
8510
8515
8520
8525
8530
8535
8540
8545
8550
8555
8560
8565
8570
8575
8580
8585
8590
8595
8600
8605
8610
8615
8620
8625
8630
8635
8640
8645
8650
8655
8660
8665
8670
8675
8680
8685
8690
8695
8700
8705
8710
8715
8720
8725
8730
8735
8740
8745
8750
8755
8760
8765
8770
8775
8780
8785
8790
8795
8800
8805
8810
8815
8820
8825
8830
8835
8840
8845
8850
8855
8860
8865
8870
8875
8880
8885
8890
8895
8900
8905
8910
8915
8920
8925
8930
8935
8940
8945
8950
8955
8960
8965
8970
8975
8980
8985
8990
8995
9000
9005
9010
9015
9020
9025
9030
9035
9040
9045
9050
9055
9060
9065
9070
9075
9080
9085
9090
9095
9100
9105
9110
9115
9120
9125
9130
9135
9140
9145
9150
9155
9160
9165
9170
9175
9180
9185
9190
9195
9200
9205
9210
9215
9220
9225
9230
9235
9240
9245
9250
9255
9260
9265
9270
9275
9280
9285
9290
9295
9300
9305
9310
9315
9320
9325
9330
9335
9340
9345
9350
9355
9360
9365
9370
9375
9380
9385
9390
9395
9400
9405
9410
9415
9420
9425
9430
9435
9440
9445
9450
9455
9460
9465
9470
9475
9480
9485
9490
9495
9500
9505
9510
9515
9520
9525
9530
9535
9540
9545
9550
9555
9560
9565
9570
9575
9580
9585
9590
9595
9600
9605
9610
9615
9620
9625
9630
9635
9640
9645
9650
9655
9660
9665
9670
9675
9680
9685
9690
9695
9700
9705
9710
9715
9720
9725
9730
9735
9740
9745
9750
9755
9760
9765
9770
9775
9780
9785
9790
9795
9800
9805
9810
9815
9820
9825
9830
9835
9840
9845
9850
9855
9860
9865
9870
9875
9880
9885
9890
9895
9900
9905
9910
9915
9920
9925
9930
9935
9940
9945
9950
9955
9960
9965
9970
9975
9980
9985
9990
9995
10000
10005
10010
10015
10020
10025
10030
10035
10040
10045
10050
10055
10060
10065
10070
10075
10080
10085
10090
10095
10100
10105
10110
10115
10120
10125
10130
10135
10140
10145
10150
10155
10160
10165
10170
10175
10180
10185
10190
10195
10200
10205

5

2

10

15

20

A network server that is located within an individual link of a network can create a problem if the server fails during network operation. That is, the failure will generally sever the connection between the nodes on either side of the network link. If a firewall device fails, for example, the two networks attached thereto will no longer be able to communicate with one another. Many times, such network links are critical to an entity's business activities and must operate without interruption. For this reason, many businesses are reluctant to install servers within these critical links. Failure to install such servers (such as, for example, a firewall) may compromise network security, which can produce equal or greater harm to the entity.

Therefore, a need exists for a method and apparatus that allows uninterrupted service through a network link having a server, even if the server fails.

25

SUMMARY

30

35

The present invention relates to a method and apparatus for providing uninterrupted communication over a network link that includes in-line processing functionality, such as a firewall device. The system includes a switch that can be used to bypass the in-line processing functionality should the functionality fail. In one embodiment, backup functionality is provided to perform the in-line processing when a failure of the original processing functionality is detected. The system also includes a controller for monitoring the in-line processing functionality and for reconfiguring the switch when a failure is detected. The invention can be advantageously implemented, for example, to provide uninterrupted, secure access to a private communications network using a firewall device or similar apparatus.

40

45

In a preferred embodiment of the invention, the switch is an Ethernet switch having virtual local access network (VLAN) capabilities. VLAN capabilities allow port groups to be defined that control how external entities connected to the switch will be interconnected with one another. In addition, switching modes can generally be defined that each include a different combination of port groupings. In accordance with the present invention, the mode of the Ethernet switch is changed when a failure of an in-line processing unit has been detected. This mode change effectively bypasses the failed unit so that communications is substantially uninterrupted.

50

55

BRIEF DESCRIPTION OF THE DRAWINGS

Figs. 1 and 2 are block diagrams illustrating typical networking arrangements between a public network and a private network;

Fig. 3 is a block diagram illustrating a system in accordance with one embodiment of the present invention;

Fig. 4 is a block diagram illustrating a system in accordance with another embodiment of the present invention;

Fig. 5 is a block diagram illustrating a system in accordance with yet another embodiment of the present invention.

DETAILED DESCRIPTION

The present invention relates to a system for providing uninterrupted service through a network link having an in-line server. That is, even if the in-line server fails, communications over the network link are not severed. Thus, the system allows servers (such as firewall devices) to be used within critical network links without fear of losing the network link. The system includes a switching device that allows the server to be bypassed if and when a server failure occurs. In a preferred embodiment, the server bypass function is automatic and operates in substantially real time so that critical communications through the link are minimally affected. The system has particular application in networks utilizing Ethernet technology.

The principles of the present invention will be described in conjunction with an Internet firewall embodiment. It should be appreciated, however, that the principles of the present invention have application in any network configuration where a first network portion is connected to a second network portion by a network link that includes an in-line server through which communications must pass. For example, in one embodiment, the inventive principles are used to provide uninterrupted communication between two subnetworks within a single network that are interconnected via a connection device within the network. It should also be noted that the figures set forth herein generally use the same reference numerals to describe the same or similar functionality.

Fig. 1 is a block diagram illustrating a typical networking scenario wherein a private network 12 is connected to a public network 10 via an inter-network connection 14. The

5

4

10

private network 12 can include, for example, a network within a corporation that allows employees of the corporation to communicate and share resources with one another. The public network 10 can include any network that can be accessed by the public, such as the Internet. The inter-network link 14 represents the communication path between the networks 10, 12 and can include, for example, a connection from the private network 12 to the Internet backbone. Such a connection can be direct or through an Internet Service Provider (ISP).

15

20

For security reasons, a manager of the private network 12 may decide that access to the private network 12 from the public network 10 is to be limited. In such cases, the manager will generally place a firewall device 16 somewhere within the inter-network link 14, as illustrated in Fig. 2. In general, a firewall device is a filter that only allows certain information to pass from an input port to an output port. All other information is generally discarded. Firewall devices can be implemented in software, hardware, or a combination of the two. Often, firewall devices are implemented using personal computers that are preprogrammed with the appropriate firewall routines. Firewall devices are generally placed "in-line" within a network link so that all communications on the link pass through the firewall device. As can be appreciated, this "in-line" configuration can create problems should the firewall device 16 fail. Most notably, such a failure could cut off all communications through the implementing network link.

25

30

35

Fig. 3 is a block diagram illustrating a system 20 for providing an uninterrupted connection between two networks in accordance with one embodiment of the present invention. It should be appreciated that the blocks shown in Fig. 3 and other block diagrams herein are functional elements that do not necessarily correspond to discrete hardware elements. For example, two or more of the associated functions may be implemented in software within a single digital processor. As illustrated, the system 20 includes a switch 22, a controller 24, and a firewall device 16 and is interposed within a inter-network link 14 between a public network 10 and a private network 12. The system 20 is capable of providing an uninterrupted connection between the public network 10 and a private network 12, regardless of the condition of the firewall device 16. The switch 22 includes a number of input/output ports for receiving and transmitting signals. At least one of the ports is connected to the public network 10, at least one is connected to the private network 12, and at least one other port is connected to the firewall device 16. The controller 24 is coupled to

40

25

45

30

50

55

5

5

the switch 22, via control line 36, for controlling the operation thereof. The controller 24 is also coupled to the firewall device 16, via sense line 40, for sensing a present operational condition of the firewall device 16.

10

During normal operation, the switch 22 is operative for directing all communications between the public network 10 and the private network 12 to the firewall device 16 for processing. If the firewall device 16 fails, however, the switch 22 provides a direct communication path between the two networks 10, 12 until the failure has been remedied. The controller 24 monitors the condition of the firewall device 16 and configures the switch 22 in accordance therewith. That is, during normal operation, the controller 24 sends information/instructions to the switch 22 that configures the switch to direct communications through the firewall device 16. When the controller 24 detects that the firewall device 16 has failed, it sends information/instructions to the switch 22 that reconfigures the switch 22 to enable a bypass of the firewall device 16. The controller 24 can then signal a network operator that the firewall device 16 needs to be repaired or replaced.

15

20

25

The controller 24 can include virtually any type of device that is capable of sensing a condition and generating an appropriate control signal in response thereto. In a preferred embodiment, the controller 24 is implemented within a digital processing device, such as a general purpose microprocessor or a digital signal processor. The controller 24 can be a separate unit from the switch 22 or it can be an integral part of a larger switch assembly. The controller 24 can sense a failure of the firewall device 16 in any of a number of different ways. For example, as shown in Fig. 3, a sense connection 40 can be provided between the controller 24 and the firewall device 16 that allows the controller 24 to directly monitor/measure one or more performance related characteristics of the firewall device 16. The controller 24 can then determine whether the firewall device 16 has failed based on these characteristics. Another method for determining whether a firewall failure has occurred involves monitoring the signals going into and out of the firewall device 16. The controller 24 can do this by monitoring, for example, the port(s) of the switch 22 that is coupled to the firewall device 16. If it is determined that nothing is being passed by the firewall device 16, it can be assumed that a failure has occurred. In one technique, the controller 24 performs a "test" on the firewall device 16 by sending a test signal into the device 16 via the switch 22. The test signal is one that should pass through the firewall device 16 in a known manner. For

30

35

40

45

50

55

5

6

10

15

example, the test signal could be a packet that should pass through the firewall device 16 and emerge with a particular destination address in a header portion. If the signal does not pass through the firewall device 16 in the expected manner, the controller 24 can use this as evidence of a failure. As can be appreciated, many other methods for detecting firewall failures can also be used in accordance with the present invention. In a preferred approach, the controller 24 will only register failures that will result in a serious reduction in throughput through the firewall device 16. That is, less serious failures that only reduce throughput slightly will be ignored.

20

25

30

The switch 22 can include any form of switch that is capable of performing the requisite bypass in response to a control signal. The switch 22 can include either mechanical or electrical switching elements or the switching function can be implemented in software. In a preferred embodiment of the invention, as illustrated in Fig. 4, an Ethernet switch 38 having virtual local area network (VLAN) capability is used. The Ethernet switch 38 has a number of input/output ports 26-29 that are used to receive/transmit information from/to attached entities. In the illustrated embodiment, a first port 26 is connected to the private network 12, a second port 27 is connected to the public network 10, and a third and fourth port 28, 29 are connected to the firewall device 16. That is, the third port 28 of the switch 38 is connected to a first port 30 of the firewall device 16 and the fourth port 29 of the switch 38 is connected to a second port 31 of the firewall device 16.

35

40

45

50

The VLAN capability of the Ethernet switch 28, in general, allows a user to define a number of different VLAN groups for the Ethernet switch 38 that control how external entities connected to the Ethernet switch 38 are interconnected through the switch 38. Each of the VLAN groups corresponds to one or more of the available input/output ports of the switch 38, thus allowing all external entities connected to those ports to communicate with one another through the switch 38. If two ports are not associated with a common VLAN group, then the external entities attached to those ports will not be able to communicate with one another through the Ethernet switch 38 (although they may be able to communicate with one another via a connection outside the Ethernet switch 38). The Ethernet switch 38 will also preferably allow switching "modes" to be defined. Each of the switching modes will consist of a different arrangement of VLAN groups. The controller 24 can then change the

55

current mode of the Ethernet switch 38 by delivering an appropriate control signal to the Ethernet switch 38 via control line 36.

In the preferred embodiment, a first switch mode is defined for use when the firewall device 16 is operating properly and a second switch mode is defined for use when the firewall device 16 has experienced a failure. In the first mode, a first VLAN group is defined that includes the second and third ports 27, 28 of the switch 38 and a second VLAN group is defined that includes the first and fourth ports 26, 29 of the switch 38. Thus, the public network 10 is linked to the first port 30 of the firewall device 16 and the private network 12 is connected to the second port 31 of the firewall device 16. Communications between the public network 10 and the private network 12 must therefore take place through the firewall device 16 which appropriately filters the communications. In the second mode, a third VLAN group is defined that includes the first port 26 and the second port 27 and a fourth VLAN group is defined that includes the fourth port 29. Thus, the public network 10 is given direct access to the private network 12 and the firewall device 16 is bypassed. It should be noted that the first and second VLAN groups will normally be deactivated when the second switch mode is enabled. It may be desirable to include the third port 28 of the Ethernet switch 38 within the third VLAN group so that users within the private network 12, for example, can monitor the condition of the firewall device 16 (e.g., determine when it is again operational). In a preferred embodiment, the controller 24 will simply indicate a mode number to the switch 38 to appropriately configure the switch 38 based on current conditions. In an alternate embodiment, the controller 24 must indicate to the switch 38 which of the switch ports are to be interconnected within each VLAN group at a particular point in time.

As can be appreciated, some private networks are not able to allow full public access to the network, even for a short period of time. For example, a corporation may maintain important business information on its network that it does not want to be accessible by its competitors. Fig. 5 is a block diagram illustrating a system 50 that is capable of providing uninterrupted, firewall-protected communication between two networks in accordance with one embodiment of the present invention. As illustrated, the system 50 is similar to the previously described embodiment with the addition of a backup firewall device 52 for use when the first firewall device 16 fails. The backup firewall device 52 includes a first port 54 that is connected to a fifth port 44 of the Ethernet switch 38 and a second port 56 that is

connected to a sixth port 46 of the Ethernet switch 38. In addition, the backup firewall device 52 can also be connected to the controller 24 via a sense line 48. The backup firewall device 52 can be identical to the first firewall device 50 or, to reduce implementation costs, a less sophisticated device may be implemented.

With reference to Fig. 5, during normal operation, the controller 24 configures the Ethernet switch 38 to direct all communications between the public network 10 and the private network 12 through the firewall device 16. When the controller 24 detects a failure of the firewall device 16, the controller 24 reconfigures the Ethernet switch 38 to all communications through the backup firewall device 52. A first mode can be defined that includes a first VLAN group comprising the second and third ports 27, 28 of the Ethernet switch 38 and a second VLAN group that includes the first and fourth ports 26, 29 of the switch 38. A second mode is defined that includes a third VLAN group comprising the second and fifth ports 27, 44 of the switch 38 and a fourth VLAN group that includes the first and sixth ports 26, 46 of the switch 38. When the controller 24 detects a failure of the first firewall device 16, it instructs the Ethernet switch 38 to change from the first switch mode to the second switch mode. The backup firewall device 52 then takes over the filtering function. When the first firewall device 16 has been repaired or replaced, the Ethernet switch 38 can be returned to the first switch mode. As can be appreciated, any number of backup firewall devices can be provided in accordance with the principles of the present invention.

Although the present invention has been described in conjunction with its preferred embodiments, it is to be understood that modifications and variations may be resorted to without departing from the spirit and scope of the invention as those skilled in the art readily understand. For example, as described previously, the principles of the invention can be used to ensure connectivity in any network situation that involves an in-line server device. This may include, for example, servers that are located between sub-networks in a single overall network. Such modifications and variations are considered to be within the purview and scope of the invention and the appended claims.

Claims

5

10

15

20

25

30

35

40

45

50

55

5

9

What is claimed is:

10

1. A system for use in providing uninterrupted communication between a first network portion and a second network portion, comprising:

5 a server unit for processing signals input into said server unit, said server unit including an output for outputting processed signals;

15

a multi-port switch having a first port connected to the first network portion, a second port connected to the second network portion, and a third port connected to said server unit; and

20

10 a controller, operatively coupled to the multi-port switch, for configuring said switch during normal operation so that communications between said first network portion and said second network portion are input into said server unit for processing, said controller including an apparatus for reconfiguring said switch, in response to a predetermined occurrence, so that communications between said first network portion and said second network portion are not input into said server unit for processing.

25

15 2. The system, as claimed in claim 1, wherein:

said predetermined occurrence includes detection of a failure of said server unit by said controller.

30

3. The system, as claimed in claim 1, wherein:

said controller includes a monitor for monitoring said server unit to determine whether

35

20 a failure has occurred within said server unit.

4. The system, as claimed in claim 1, wherein:

said server unit includes a firewall machine.

5. The system, as claimed in claim 1, wherein:

40

said multi-port switch includes an Ethernet switch having virtual local access network

25 (VLAN) functionality

6. The system, as claimed in claim 1, wherein:

said controller includes a digital processing unit.

45

7. The system, as claimed in claim 1, wherein:

said controller is integrally associated with said multi-port switch.

30

8. The system, as claimed in claim 7, wherein:

said controller is located within a housing of said multi-port switch.

50

55

5

10

9. The system, as claimed in claim 1, further comprising:
a backup server unit coupled to a fourth port of said multi-port switch.

10

10. The system, as claimed in claim 9, wherein:

said apparatus for reconfiguring said switch reconfigures said switch so that
5 communications between said first network portion and said second network portion are input
into said backup server unit for processing.

15

11. The system, as claimed in claim 1, wherein:

said apparatus for reconfiguring said switch reconfigures said switch so that
communications between said first network portion and said second network portion are
20 transferred without processing within said system.

20

12. The system, as claimed in claim 1, wherein:

said first network portion is located within a first network and said second network
portion is located within a second network, wherein said second network is different from said
25 first network.

25

15 13. The system, as claimed in claim 1, wherein:

said first network portion and said second network portion are both subnetworks of
30 a common network.

30

14. A system for use in providing uninterrupted communication between a first
network portion and a second network portion, said system comprising:

35

20 a switch having a plurality of ports, wherein a first of said plurality of ports is coupled
to the first network portion and a second of said plurality of ports is coupled to the second
network portion, said switch permitting port groups to be defined that each include a subset
of said plurality of ports, wherein two external entities are only capable of directly
40 communicating with each other through said switch if the two external entities are each
connected to respective ports of said switch that are within a common port group, said switch
having a first configuration comprising first and second port groups and a second
configuration comprising a third port group, wherein said third port group is different from
45 said first and second port groups;

45

a server unit having a first server port and a second server port, said first server port
30 being connected to a third of said plurality of ports and said second server port being

50

55

connected to a fourth of said plurality of ports, wherein said server unit is operative for processing signals propagating between said first server port and said second server port; and

a controller, coupled to said switch, for changing a configuration of said switch from said first configuration to said second configuration in response to a predetermined occurrence.

15. The system, as claimed in claim 14, wherein:

said first port group includes said second port and said third port of said switch and said second port group includes said first port and said fourth port of said switch.

16. The system, as claimed in claim 15, wherein:

said third port group includes said first port and said second port of said switch.

17. The system, as claimed in claim 15, further comprising:

a backup server unit having a third server port and a fourth server port, said third server port being connected to a fifth of said plurality of ports and said fourth server port being connected to a sixth of said plurality of ports, wherein said backup server unit is operative for processing signals propagating between said third server port and said fourth server port;

wherein said third port group includes said second port and said fifth port of said switch, said second configuration further comprising a fourth port group including said first port and said sixth port of said switch.

18. The system, as claimed in claim 14, wherein:

said switch includes an Ethernet switch having virtual local area network (VLAN) capability.

19. The system, as claimed in claim 18, wherein:

each of said port groups comprises an individual VLAN grouping.

20. The system, as claimed in claim 14, wherein:

said predetermined occurrence includes detection of a failure of said server unit.

21. The system, as claimed in claim 14, wherein:

said server unit includes a firewall machine for use in filtering signals flowing therethrough.

22. The system, as claimed in claim 14, wherein:

said controller is not accessible from at least one of said first network portion and said second network portion.

23. The system, as claimed in claim 14, wherein:

said third port group further comprises said third port of said switch.

24. A method for use in providing secure access to a first network portion from a second network portion utilizing an Ethernet switch, said Ethernet switch having at least three ports, a first port being connected to the first network portion, a second port being connected to second network portion, and at least one port being connected to a firewall machine, said firewall machine including an ability to filter signals that are input into said firewall machine so that only authorized signals are allowed to pass to an output of said firewall machine, said method comprising the steps of:

first configuring said Ethernet switch so that communications flowing between the first and second network portions are directed through the firewall machine for processing;

monitoring said firewall machine to detect failures within said firewall machine; and second configuring said Ethernet switch, when a failure has been detected in said firewall machine, so that communications flowing between the first and second networks bypass the firewall machine.

25. The method, as claimed in claim 24, wherein:

said Ethernet switch includes virtual local area network (VLAN) functionality, wherein said at least one port includes a third port and a fourth port connected to said firewall machine; and

said step of first configuring includes enabling a first VLAN grouping and a second VLAN grouping, wherein said first VLAN grouping includes said second port and said third port and said second VLAN grouping includes said first port and said fourth port.

26. The method, as claimed in claim 25, wherein:

said step of second configuring includes enabling a third VLAN grouping including said first port and said second port of said switch.

27. The method, as claimed in claim 26, wherein:

said third VLAN grouping includes at least one of said third port and said fourth port.

5

13

28. The method, as claimed in claim 24, further comprising:

10

providing a backup firewall machine that is coupled to at least one fifth port of said Ethernet switch, wherein said step of second configuring includes configuring said Ethernet switch so that communications flowing between the first and second network portions are

5 directed through the backup firewall machine for processing.

15

20

25

30

35

40

45

50

55

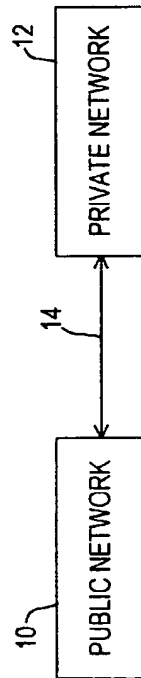


FIG. 1

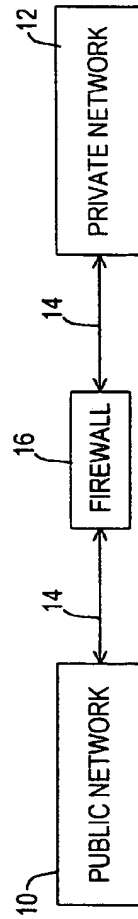


FIG. 2

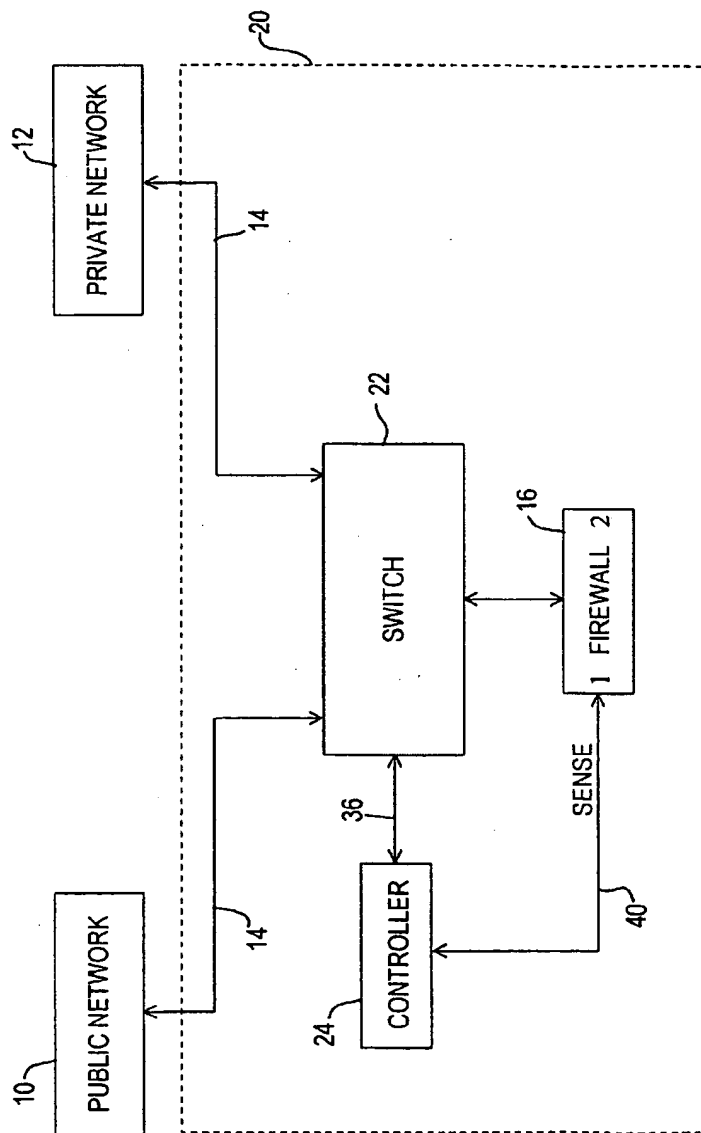


FIG. 3

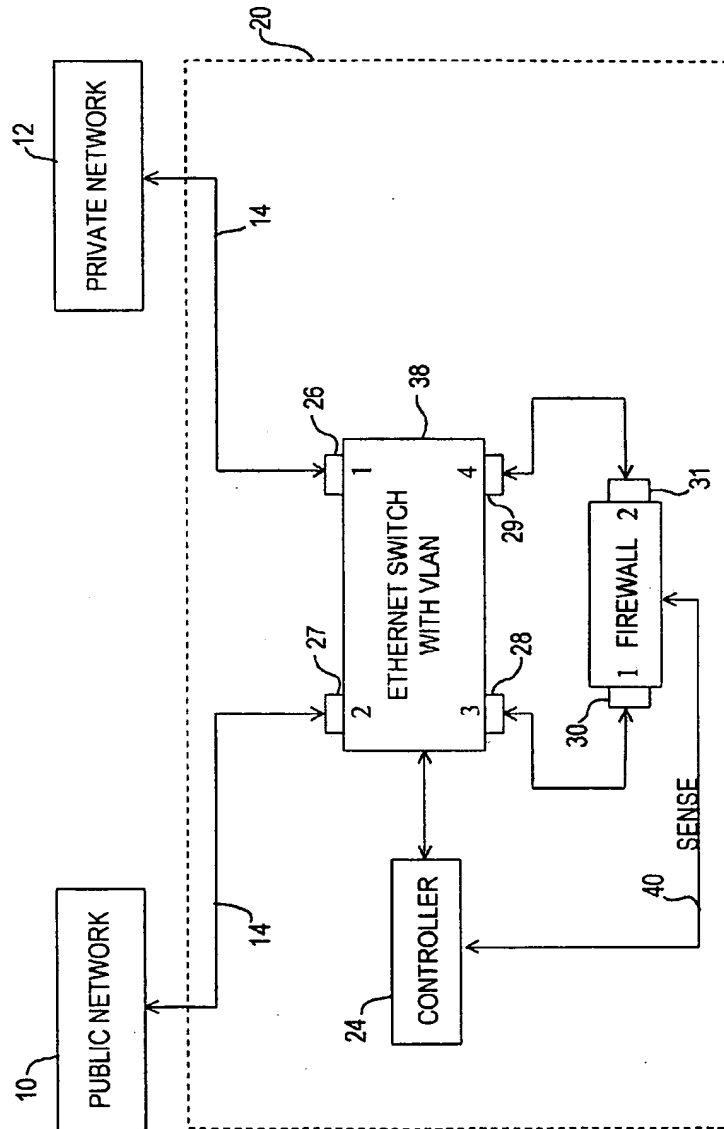


FIG. 4

4/4

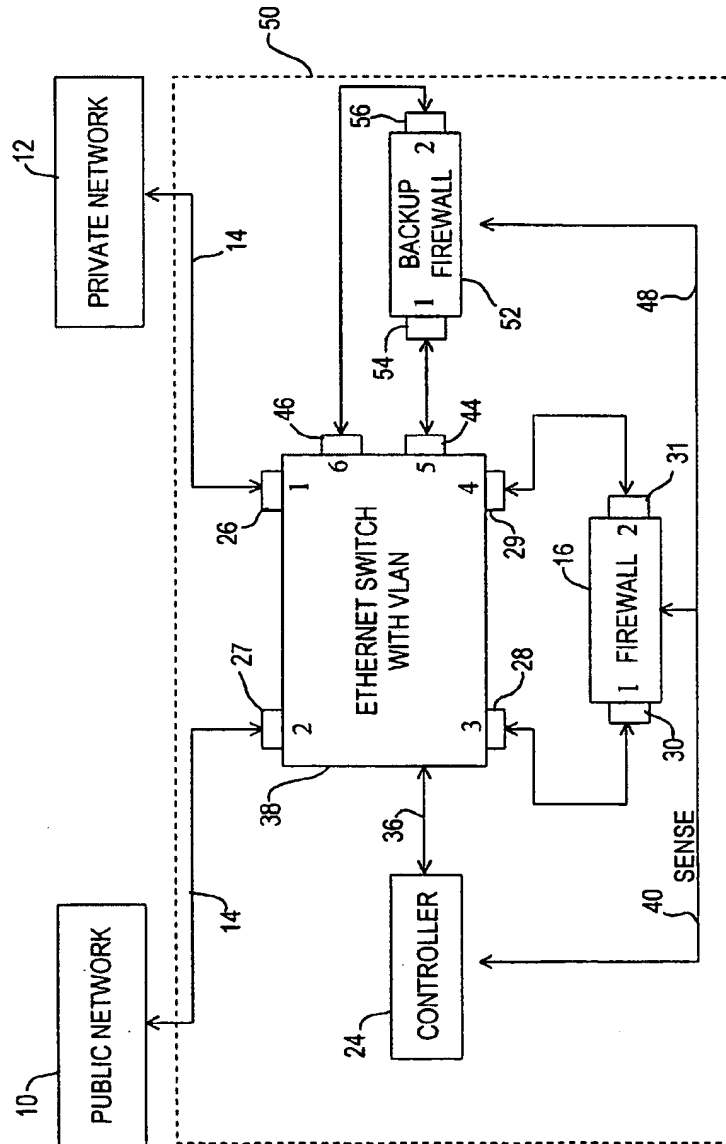


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/05086

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H02H 3/05; H04L 1/22; G06F 15/177
US CL : 714/48, 47; 713/201; 709/220, 221, 224, 249

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 714/48, 47; 713/201; 709/220, 221, 224, 249

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PLUS, STN. EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	UA 5,802,320 A [BEAHR et al.] 01 September 1998, see abstract, fig.5, col.3, line 15 through col.6, line 18, col.7, line 12 through col.8, line 68, col.9, line 8 through col.10, line 45	1-28
Y	US 5,790,548 A [SISTANIZADEH et al.] 04 August 1998, see abstract, fig.10, col.1, lines 62-68, col.8, lines 3-9, col.12, lines 3-20	1-28
A	US 5,473,599 A [LI et al.] 05 December 1995, see entire document	1-28
A	US 5,287,461 A [MOORE] 15 February 1994, see entire document	1-28

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* "Special categories of cited documents:	* "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
* "A" document defining the general state of the art which is not considered to be of particular relevance	* "X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
* "B" earlier document published on or after the international filing date	* "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
* "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	* "G" document member of the same patent family
* "O" document referring to an oral disclosure, use, exhibition or other means	
* "P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

09 JUNE 2000

Date of mailing of the international search report

27 JUN 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized Officer

DIEU-MINH LE

Telephone No. (703) 305-9408

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/05086

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,432,907 A [PICAZO, Jr. et al.] 11 July 1995, see entire document	1-28
A	US 5,781,715 A [SHEU] 14 July 1998, see entire document	1-28